(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6426520号
(P6426520)

(45)発行日　平成30年11月21日(2018.11.21)　(24)登録日　平成30年11月2日(2018.11.2)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601A
H04L 9/32	(2006.01)	H04L	9/00	675D
G06F 21/31	(2013.01)	G06F	21/31	
G06F 21/62	(2013.01)	G06F	21/62	
H04L 9/14	(2006.01)	H04L	9/00	673A

請求項の数 5　(全 16 頁)　最終頁に続く

(21)出願番号　特願2015-72484(P2015-72484)
(22)出願日　平成27年3月31日(2015.3.31)
(65)公開番号　特開2016-192715(P2016-192715A)
(43)公開日　平成28年11月10日(2016.11.10)
審査請求日　平成30年1月18日(2018.1.18)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(73)特許権者　301063496
東芝デジタルソリューションズ株式会社
神奈川県川崎市幸区堀川町７２番地３４
(74)代理人　110000235
特許業務法人　天城国際特許事務所
(72)発明者　和田　敏治
神奈川県川崎市幸区堀川町７２番地３４
東芝ソリューション株式会社内
(72)発明者　大畑　文明
神奈川県川崎市幸区堀川町７２番地３４
東芝ソリューション株式会社内

最終頁に続く

(54)【発明の名称】暗号鍵管理システムおよび暗号鍵管理方法

(57)【特許請求の範囲】
【請求項１】
マスター鍵により保護データを暗号化および復号化するサーバと、
ユーザＩＤおよびパスワードを含む入力情報に基づいて前記サーバにユーザ認証を要求するとともに、前記保護データの暗号化および復号化を要求するユーザ端末と、を備え、
前記サーバが、
前記ユーザＩＤ、前記パスワードから算出されたパスワードハッシュ、および前記パスワードハッシュのリビジョンを関連付けたユーザ情報を記憶するユーザ情報記憶手段と、
前記ユーザＩＤ、前記パスワードから算出された鍵ハッシュにより前記マスター鍵を暗号化した暗号化済鍵、および前記リビジョンを関連付けた鍵情報を記憶する鍵情報記憶手段と、
前記入力情報と前記ユーザ情報とを照合して前記ユーザ認証が完了した場合に、認証ＩＤを発行するとともに、この認証ＩＤに対して、前記ユーザＩＤ、前記リビジョン、前記鍵ハッシュ、および認証時刻を関連付けた認証情報を生成し、保持する認証手段と、
前記パスワードを新たなパスワードへ変更する場合に、前記認証情報に含まれる前記ユーザＩＤと前記リビジョンの組合せを検索キーとして前記鍵情報から取得した前記暗号化済鍵を、前記鍵ハッシュで復号して前記マスター鍵を取得するとともに、前記新たなパスワードと前記マスター鍵に基づいて新たな暗号化済鍵を作成し、前記ユーザＩＤ、前記新たなパスワードに係る新たなリビジョン、および前記新たな暗号化済鍵を関連付けた新たな鍵情報を同一の前記ユーザＩＤに係る他の鍵情報と併存した状態で前記鍵情報記憶手段

へ保存する鍵再暗号化手段と、
を有することを特徴とする暗号鍵管理システム。
【請求項２】
前記鍵再暗号化手段は、前記ユーザ端末側から共通の前記認証ＩＤに対して認証時と異なる他のユーザＩＤおよび他のパスワードを関連付けるパスワード変更要求があった場合に、前記他のパスワードから他の鍵ハッシュを生成するとともに、前記認証情報から共通の前記認証ＩＤに関連付けられている前記ユーザＩＤ、前記鍵ハッシュを取得して前記マスター鍵を復号し、このマスター鍵により前記他の鍵ハッシュを暗号化した他の暗号化済鍵、前記他のユーザＩＤ、および前記他のパスワードのリビジョンを組み合わせた他の鍵情報を前記鍵情報記憶手段に保存することを特徴とする請求項１記載の暗号鍵管理システム。
【請求項３】
前記鍵情報記憶手段内に記憶されている鍵情報に含まれる前記ユーザＩＤおよび前記リビジョンの組合せが前記認証手段内に保持されている前記認証情報の中に存在しない場合に、前記存在しない組合せに対応する前記鍵情報を前記鍵情報記憶手段から削除する鍵掃除手段を更に備えることを特徴とする請求項１または請求項２記載の暗号鍵管理システム。
【請求項４】
前記サーバは、前記認証手段、前記鍵再暗号化手段、前記ユーザ情報記憶手段および前記鍵情報記憶手段を２以上のコンピュータに分散配置し、ネットワークを介して互いに接続することで構成されている請求項１乃至請求項３のいずれか一項記載の暗号鍵管理システム。
【請求項５】
マスター鍵により保護データを暗号化および復号化するサーバと、ユーザＩＤおよびパスワードを含む入力情報に基づいて前記サーバにユーザ認証を要求するとともに、前記保護データの暗号化および復号化を要求するユーザ端末と、からなるコンピュータシステムにおける暗号鍵管理方法であって、
前記サーバが、前記ユーザＩＤ、前記パスワードから算出されたパスワードハッシュ、および前記パスワードハッシュのリビジョンを関連付けたユーザ情報を記憶領域へ記憶するユーザ情報記憶ステップと、
前記ユーザＩＤ、前記パスワードから算出された鍵ハッシュにより前記マスター鍵を暗号化した暗号化済鍵、および前記リビジョンを関連付けた鍵情報を前記記憶領域へ記憶する鍵情報記憶ステップと、
前記入力情報と前記ユーザ情報とを照合して前記ユーザ認証が完了した場合に、認証ＩＤを発行するとともに、この認証ＩＤに対して、前記ユーザＩＤ、前記リビジョン、前記鍵ハッシュ、および認証時刻を関連付けた認証情報を生成し、保持する認証ステップと、
前記ユーザ認証で入力された前記パスワードを新たなパスワードへ変更する場合に、前記認証情報に含まれる前記ユーザＩＤと前記リビジョンの組合せを検索キーとして前記鍵情報から取得した前記暗号化済鍵を、前記認証情報に含まれる前記鍵ハッシュで復号して前記マスター鍵を取得するとともに、前記新たなパスワードと前記マスター鍵に基づいて新たな暗号化済鍵を作成し、前記ユーザＩＤ、前記新たなパスワードに係る新たなリビジョン、および前記新たな暗号化済鍵を関連付けた新たな鍵情報を同一の前記ユーザＩＤに係る他の鍵情報と併存した状態で前記記憶領域へ保存する鍵再暗号化ステップと、
を有することを特徴とする暗号鍵管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本実施形態は、暗号鍵管理システムおよび暗号鍵管理方法
に関する。
【背景技術】

【０００２】
近年、個人情報などの秘匿したい情報（以下、秘匿情報という。）について、ユーザ認証により情報を保護できるだけでなく、データベースの複製やＨＤＤの抜き取り（２次記憶の詐取）、又はバックアップメディアの盗難（３次記憶の詐取）など、２次記憶や３次記憶に保存された情報が詐取された場合あっても秘匿情報を保護できるシステムが求められている。
【０００３】
このような要求に対し、データサーバ側で秘匿情報を暗号化して保存し、その暗号化に使用した暗号鍵をアプリケーションサーバ側に保存するシステムなどが知られているが、両サーバの２次記憶の情報が詐取されてしまうと、暗号化された秘匿情報を暗号鍵で復号することが可能になってしまう。
【０００４】
そこで、システムを利用するユーザ自身しか知り得ない情報（例えばパスワード）から作成した暗号鍵（鍵ハッシュ）をシステム内に保存する手法が有効となっている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１２－７９２３１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、従来技術においては、ユーザが認証後にシステムを利用しながら、並行してパスワードを変更した場合には、認証時に作成した暗号鍵（以下、旧暗号鍵という。）と、パスワード変更によって新たに作成された暗号鍵（以下、新暗号鍵という。）の内容が異なってしまう。この結果、旧暗号鍵を用いて秘匿された情報（保護データ）を新暗号鍵で復号しようとすると失敗してしまうため、復号時のエラーを回避するためには再認証を行った上で新暗号鍵を作成しなければならず、作業効率の低下を招くという問題があった。
【０００７】
そこで、本発明は、上記従来技術の問題に鑑み、認証されたユーザがシステムを利用している際に、並行してパスワードの変更があった場合に、再認証を実行することなく、パスワード変更前の旧暗号鍵によって暗号化された保護データを継続して復号可能にするものである。
【課題を解決するための手段】
【０００８】
本実施形態の暗号鍵管理システムは、マスター鍵により保護データを暗号化および復号化するサーバと、ユーザＩＤおよびパスワードを含む入力情報に基づいて前記サーバにネットワークを介してユーザ認証を要求するとともに、前記保護データの暗号化および復号化を要求するユーザ端末と、を備える暗号鍵管理システムであって、前記サーバが、前記ユーザＩＤ、前記パスワードから算出されたパスワードハッシュ、および前記パスワードハッシュのリビジョンを関連付けたユーザ情報を記憶するユーザ情報記憶手段と、前記ユーザＩＤ、前記パスワードから算出された鍵ハッシュにより前記マスター鍵を暗号化した暗号化済鍵、および前記リビジョンを関連付けた鍵情報を記憶する鍵情報記憶手段と、前記入力情報と前記ユーザ情報とを照合して前記ユーザ認証が完了した場合に、認証ＩＤを発行するとともに、この認証ＩＤに対して、前記ユーザＩＤ、前記リビジョン、前記鍵ハッシュ、および認証時刻を関連付けた認証情報を生成し、保持する認証手段と、前記パスワードを新たなパスワードへ変更する場合に、前記認証情報に含まれる前記ユーザＩＤと前記リビジョンの組合せを検索キーとして前記鍵情報から取得した前記暗号化済鍵を、前記鍵ハッシュで復号して前記マスター鍵を取得するとともに、前記新たなパスワードと前記マスター鍵に基づいて新たな暗号化済鍵を作成し、前記ユーザＩＤ、前記新たなパスワ

ードに係る新たなリビジョン、および前記新たな暗号化済鍵を関連付けた新たな鍵情報を同一の前記ユーザＩＤに係る他の鍵情報と併存した状態で前記鍵情報記憶手段へ保存する鍵再暗号化手段と、を有することを特徴とする。

【図面の簡単な説明】

【０００９】

【図１】一実施形態に係る暗号鍵管理システムの全体構成の一例を示すブロック図。

【図２】認証情報の一例を示す図。

【図３】ユーザ情報の一例を示す図。

【図４】鍵情報の一例を示す図。

【図５】保護データの一例を示す図。

【図６】ユーザ認証処理の説明図。

【図７】保護データ登録処理の説明図。

【図８】保護データ取得処理の説明図。

【図９】同一ユーザの要求によるパスワード変更処理の説明図。

【図１０】他のユーザの要求によるパスワード変更処理の説明図。

【図１１】認証維持処理の説明図。

【図１２】鍵情報掃除処理の説明図。

【図１３】認証情報削除処理の説明図。

【図１４】一実施形態に係る暗号鍵管理システムにおけるパスワード変更時の動作の一例を示すシーケンス図。

【発明を実施するための形態】

【００１０】

以下、本実施形態に係る暗号鍵管理システムについて図面を参照して詳細に説明する。

【００１１】

図１は、一実施形態に係る暗号鍵管理システムの全体構成の一例を示すブロック図である。同図に示されるように、暗号鍵管理システムは、ユーザ端末１、認証サーバ２、ユーザＤＢ３、アプリケーションサーバ４、およびデータサーバ５が通信ネットワークＮＷを介して接続されることで構成されている。

【００１２】

各装置は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、入力装置、表示装置、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）などの大容量の記憶装置、および通信装置などから構成されたコンピュータであり、台数はそれぞれ任意である。また、本システムでは複数台のサーバを含んでいるが、一台あるいは複数台のサーバに適宜統合あるいは分散した上でネットワーク接続してもよい。

【００１３】

ユーザ端末１は、ユーザがデータ編集作業などに用いるパーソナルコンピュータなどの情報端末であり、認証依頼手段１１、データ参照依頼手段１２、データ登録依頼手段１３、パスワード変更依頼手段１４を有している。

【００１４】

認証依頼手段１１は、認証サーバ２に対してユーザＩＤおよびパスワードを含む入力情報を送信し、ユーザ認証処理を要求する。データ参照依頼手段１２は、ユーザ認証の完了後、認証情報に基づいてアプリケーションサーバ４に接続し、データサーバ５内で管理されている保護データの参照処理を要求する。

【００１５】

データ登録依頼手段１３は、認証情報に基づいてアプリケーションサーバ４に接続し、データサーバ５へ保護データの登録処理を要求する。パスワード変更依頼手段１４は、認証サーバ２に対して既存のパスワードから新たなパスワードへの変更処理を要求する。

【００１６】

認証サーバ２は、認証処理を実行するサーバコンピュータであり、認証情報提供手段２

２、パスワード変更手段２３、認証維持手段２４、認証情報確認手段２５、鍵掃除手段２６、認証削除手段２７を有している。

【００１７】

認証手段２１は、入力情報に含まれるユーザＩＤおよびパスワードから算出した新たなパスワードハッシュを、ユーザＤＢ３が記憶するユーザ情報と照合してユーザ認証を行う。認証手段２１は、ユーザ認証が完了（成功）した場合に、固有の認証ＩＤを発行するとともに、この認証ＩＤに対して、ユーザごとに固有なユーザＩＤ、パスワードの世代番号であるリビジョン、鍵ハッシュ、および認証時刻を関連付けた認証情報を生成し、保持する。尚、鍵ハッシュは、所定のハッシュ関数を用いて算出するものとする。

【００１８】

図２は、認証情報の一例を示す図である。ここでは、認証情報が、認証ＩＤごとに、ユーザＩＤ、リビジョン、鍵ハッシュ、最後に認証情報にアクセスした時刻を関連付けた情報であることが示されている。鍵ハッシュは、鍵用のハッシュ関数Hk(x)を用いて算出する。ハッシュ関数Hk(x)のｘとしては、パスワードの平文Pn_m（n:ユーザ番号,m:リビジョン番号）が使用されている。

【００１９】

認証情報提供手段２２は、アプリケーションサーバ４から認証ＩＤを受信した場合に、当該認証ＩＤの認証情報をアプリケーションサーバ４に提供する。

パスワード変更手段２３は、ユーザ端末１からパスワードの変更要求があった場合に、ユーザＩＤ、新たなパスワードから算出したパスワードハッシュ、およびパスワードのリビジョンからなる新たなユーザ情報をユーザＤＢ３に送信し、ユーザ情報を更新する。また、パスワード変更手段２３は、ユーザＩＤ、現時点のパスワードのリビジョンと鍵ハッシュ、新たなパスワードに基づく鍵ハッシュをユーザＤＢ３へ送信し、新たな鍵情報の登録を行う。

【００２０】

認証維持手段２４は、アプリケーションサーバ４が保持する認証情報の認証ＩＤを受信した場合に、受信した認証ＩＤに基づいて認証サーバ２内で保持する認証情報を検索し、認証ＩＤが一致する認証情報の時刻を現在時刻に更新することで認証を維持する。

認証情報確認手段２５は、鍵掃除手段２６から受信したユーザＩＤとリビジョンの組合せ情報に対応する認証情報が認証サーバ２内に存在するか否かを確認し、組合せごとの確認結果を鍵掃除手段２６へ送信する。

【００２１】

鍵掃除手段２６は、ユーザＤＢ３が記憶する鍵情報を参照して、ユーザＩＤとリビジョンの組合せ情報を抽出し、認証情報確認手段２５へ定期的に送信する。そして、鍵掃除手段２６は、認証情報確認手段２５からの応答情報として、認証サーバ２内に存在しない鍵情報があった場合には、この鍵情報を削除する。

認証削除手段２７は、認証サーバ２側で保持している認証情報の時刻と現在時刻を定期的に比較し、所定のタイムアウト時間が経過した認証情報を削除する。

【００２２】

ユーザＤＢ３は、認証サーバ２における認証処理、データサーバ５におけるデータ書込み・読取処理にそれぞれ必要な情報を記憶するデータベースであり、ユーザ情報記憶手段３１、鍵情報記憶手段３２、鍵再暗号化手段３３を有している。

【００２３】

ユーザ情報記憶手段３１は、ユーザを特定するユーザＩＤ、パスワードハッシュ、リビジョンを関連付けたユーザ情報を記憶する。図３は、ユーザ情報の一例を示す図である。パスワードハッシュは、パスワード用のハッシュ関数Hp(x)を用いて算出する。ハッシュ関数Hp(x)のｘとしては、パスワードの平文Pn_m（n:ユーザ番号,m:リビジョン番号）が使用されている。

【００２４】

鍵情報記憶手段３２は、ユーザＩＤ、リビジョン、および暗号化済鍵を関連付けた鍵情

報を記憶する。図４は、鍵情報の一例を示す図である。暗号化済鍵は、鍵用の関数Ck(x,y)を用いて算出されている。ここでは、関数Ck(x,y)のxには鍵ハッシュ、ｙにはマスター鍵（共通鍵）Ｍが使用されている。

【００２５】

鍵再暗号化手段３３は、ユーザ認証で入力されたパスワードを新たなパスワードへ変更する場合に、認証情報に含まれるユーザＩＤとリビジョンの組合せを検索キーとして鍵情報から取得した暗号化済鍵を、認証情報に含まれる鍵ハッシュで復号してマスター鍵を取得するとともに、新たなパスワードとマスター鍵に基づいて新たな暗号化済鍵を作成し、ユーザＩＤ、新たなパスワードに係る新たなリビジョン、および新たな暗号化済鍵を関連付けた新たな鍵情報を同一のユーザＩＤに係る他の鍵情報と併存した状態で鍵情報記憶手段３２へ保存する。

【００２６】

また、鍵再暗号化手段３３は、ユーザ端末１側から共通の認証ＩＤに対して認証時と異なる他のユーザＩＤおよび他のパスワードを関連付けるパスワード変更要求があった場合に、他のパスワードから他の鍵ハッシュを生成するとともに、認証サーバ２に保持されている認証情報から共通の認証ＩＤに関連付けられているユーザＩＤ、鍵ハッシュを取得してマスター鍵を復号し、このマスター鍵により他の鍵ハッシュを暗号化した他の暗号化済鍵、他のユーザＩＤ、および他のパスワードのリビジョンを組み合わせた他の鍵情報を鍵情報記憶手段３２に保存する。

【００２７】

アプリケーションサーバ４は、種々のアプリケーション（図示省略する）の実行によりユーザ端末１に対してサービスを提供するサーバコンピュータであり、データ登録手段４１、認証情報参照手段４２、データ参照手段４３、認証維持依頼手段４４、認証削除手段４５を有している。

【００２８】

データ登録手段４１は、認証済みのユーザ端末１からデータ登録要求があった場合に、受信データをデータサーバ５へ登録する。

認証情報参照手段４２は、アプリケーションの実行に伴って認証情報が必要になった場合に、認証サーバ２に対して認証情報の参照を要求する。

【００２９】

データ参照手段４３は、認証済みのユーザ端末１からデータ参照要求があった場合に、データサーバ５から保護データを取得し、ユーザ端末１へ返信する。

認証維持依頼手段４４は、アプリケーションサーバ４側で保持している認証情報の認証ＩＤを認証サーバ２へ定期的に送信し、認証維持を要求する。認証削除手段４５は、アプリケーションサーバ４側で保持している認証情報の時刻と現在時刻を定期的に比較し、所定のタイムアウト時間が経過した認証情報を削除する。

【００３０】

データサーバ５は、保護データを管理するサーバコンピュータであり、保護データ記憶手段５１、データ書込手段５２、データ読取手段５３を有している。

【００３１】

保護データ記憶手段５１は、ユーザ端末１からアプリケーションサーバ４を介して登録要求のあった保護データを暗号化してデータＩＤごとに記憶する。図５は、保護データの一例を示す図である。ここでは、保護データを特定するデータＩＤに対して保護データをカラムごとにデータ用の関数Cd(x,y)により暗号化して関連付けて記憶している。ここでは、関数Cd(x,y)のｘはマスター鍵Ｍ、ｙはDn_mデータの平文（n:データ番号,m:カラム）となっている。

【００３２】

データ書込手段５２は、ユーザ端末１からアプリケーションサーバ４を介して取得したデータを鍵情報から復号したマスター鍵により暗号化し、これを保護データとして保護データ記憶手段５１に書き込む。データ読取手段５３は、保護データ記憶手段５１から暗号

化された保護データを読取り、鍵情報の暗号化済鍵から復号したマスター鍵で復号してアプリケーションサーバ４へ送信する。

【００３３】

続いて、暗号鍵管理システムを構成する装置間の処理の流れを具体的に説明する。

（１）ユーザ認証処理

図６は、ユーザ認証処理の説明図である。同図に示されるように、ユーザが、ユーザ端末１の認証依頼手段１１を用いて、ユーザＩＤ[U1]とパスワード[P1_1]を入力すると、ユーザ端末１は、認証サーバ２の認証手段２１に対して、ユーザＩＤ[U1]、パスワード[P1_1]とともに認証を要求する。

【００３４】

認証手段２１は、ユーザＩＤ[U1]、及びパスワード[P1_1]から生成したパスワードハッシュ[Hp(P1_1)]を、ユーザＤＢ３が保持するユーザ情報と突き合わせることにより、ユーザを認証する。ユーザ情報には、ユーザＩＤ[U1]、パスワードハッシュ[Hp(P1_1)]のほか、パスワードハッシュの更新回数を表す、リビジョン[R1]を持つ。

【００３５】

認証に成功すると、認証手段２１は、認証処理毎に付与する認証ID[A1]、ユーザＩＤ[U1]、リビジョン[R1]、認証時刻[T1]、パスワード[P1_1]から生成した鍵ハッシュ[Hk(P1_1)]の組を認証情報に新規追加し、認証ID[A1]を認証依頼手段１１に応答する。

【００３６】

（２）保護データ登録処理

図７は、保護データ登録処理の説明図である。同図に示されるように、ユーザが、ユーザ端末１のデータ登録依頼手段１３を用いて、認証ID[A1]とともに、登録データキー[D1]、登録データ値[D1_1]、[D1_2]を入力すると、ユーザ端末１は、アプリケーションサーバ４のデータ登録手段４１に対して、認証ID[A1]、登録データキー[D2]、登録データ値[D2_1]、[D2_2]とともにデータ登録を要求する。

【００３７】

データ登録手段４１は、認証情報参照手段４２に認証ID[A1]を与えることにより、認証サーバ２の認証情報提供手段２２を介して、認証ID[A1]に紐付く、ユーザＩＤ[U1]、リビジョン[R1]、鍵ハッシュ[Hk(P1_1)]を取得し、アプリケーションサーバ４内の認証情報にそれらを新規追加する。

【００３８】

次に、データ登録手段４１は、データサーバ５のデータ書込手段５２に対して、ユーザＩＤ[U1]、リビジョン[R1]、鍵ハッシュ[Hk(P1_1)]、登録データキー[D2]、登録データ値[D2_1]、[D2_2]を与え、保護データの登録を要求する。

【００３９】

データ書込手段５２は、ユーザＤＢ３が保持する鍵情報の中から、ユーザＩＤ[U1]、リビジョン[R1]に紐付く、暗号化済鍵[Ck(Hk(P1_1),M)]を取得し、鍵ハッシュ[Hk(P1_1)]を用いてマスター鍵[M]を復号する。

【００４０】

次に、データ書込手段５２は、マスター鍵[M]を用いて登録データ値[D2_1]、[D2_2]を暗号化し、それぞれ[Cd(M, D2_1)]、[Cd(M, D2_2)]として保護データに登録する。

【００４１】

（３）保護データ取得処理

図８は、保護データ取得処理の説明図である。同図に示されるように、ユーザが、ユーザ端末１のデータ参照依頼手段１２を用いて、認証ID[A1]とともに、参照データキー[D1]を入力すると、ユーザ端末１は、アプリケーションサーバ４のデータ参照手段４３に対し、認証ID[A1]、参照データキー[D1]とともにデータ参照を要求する。

【００４２】

データ参照手段４３は、認証情報参照手段４２に認証ID[A1]を与えることにより、認証サーバ２の認証情報提供手段２２を介して、認証ID[A1]に紐付く、ユーザＩＤ[U1]、リビ

ジョン[R1]、鍵ハッシュ[Hk(P1_1)]を取得し、アプリケーションサーバ４内の認証情報にそれを新規追加する。

【００４３】

次に、データ参照手段４３は、データサーバ５のデータ読取手段５３に対して、ユーザＩＤ[U1]、リビジョン[R1]、鍵ハッシュ[Hk(P1_1)]、参照データキー[D1]を与え、保護データの参照を要求する。

【００４４】

データ読取手段５３は、ユーザＤＢ３が保持する鍵情報の中から、ユーザＩＤ[U1]、リビジョン[R1]に紐付く、暗号化済鍵[Ck(Hk(P1_1),M)]を取得し、鍵ハッシュ[Hk(P1_1)]を用いてマスター鍵[M]を復号する。次に、データ読取手段５３は、マスター鍵[M]を用いて保護データが保持する[Cd(M, D1_1)]、[Cd(M, D1_2)]を復号し、それぞれ参照データ値[D1_1]、[D1_2]としてデータ参照手段４３に応答する。最後に、データ参照手段４３は、受け取った参照データ値[D1_1]、[D1_2]をデータ参照依頼手段１２に応答する。

【００４５】

（４）第１のパスワード変更処理

図９は、同一ユーザの要求によるパスワード変更処理の説明図である。同図に示されるように、ユーザが、ユーザ端末１のパスワード変更依頼手段１４を用いて、認証ID[A1]とともに、ログインユーザ自身のユーザＩＤ（以下、自ユーザＩＤという。）[U1]、新パスワード[P1_2]を入力すると、ユーザ端末１は、認証サーバ２のパスワード変更手段２３に対し、認証ID[A1]、ユーザＩＤ[U1]、[P1_2]とともにパスワード変更を要求する。

【００４６】

パスワード変更手段２３は、自身が保持する認証情報の中から、認証ID[A1]に紐付く、自ユーザＩＤ[U1]、変更前のパスワード（以下、旧パスワードという。）のリビジョン（以下、旧リビジョンという。）[R1]、旧パスワード[P1_1]から生成した鍵ハッシュ[Hk(P1_1)]を取得し、さらに[P1_2]から鍵ハッシュ[Hk(P1_2)]を生成する。

【００４７】

次に、パスワード変更手段２３は、ユーザＤＢ３の鍵再暗号化手段３３に対して、ユーザＩＤ[U1]、リビジョン[R1]、鍵ハッシュ[Hk(P1_1)]、ユーザＩＤ[U1]、鍵ハッシュ[Hk(P1_2)]を与え、マスター鍵[M]の再暗号化を要求する。

【００４８】

鍵再暗号化手段３３は、ユーザＤＢ３が保持する鍵情報の中から、ユーザＩＤ[U1]、リビジョン[R1]に紐付く、旧暗号化済鍵[Ck(Hk(P1_1),M)]を取得し、鍵ハッシュ[Hk(P1_1)]を用いてマスター鍵[M]を復号する。また、ユーザＩＤ[U1]に紐付くリビジョンのうち、最新の旧リビジョン[R1]を取得する。

【００４９】

次に、鍵再暗号化手段３３は、マスター鍵[M]を[Hk(P1_2)]を用いて暗号化し、生成された新暗号化済鍵[Ck(Hk(P1_2),M)]、ユーザＩＤ[U1]、及び新リビジョン[R2]を鍵情報に新規追加する。

【００５０】

最後に、パスワード変更手段２３は、ユーザＤＢ３が保持するユーザ情報に存在する、ユーザＩＤ[U1]に紐付くリビジョン[R1]、パスワードハッシュ[Hp(P1_1)]を、鍵再暗号化手段３３から応答として受け取ったリビジョン[R2]、新パスワード[P1_2]から生成したパスワードハッシュ[Hp(P1_2)]で上書更新し、パスワード変更依頼手段１４に応答する。

【００５１】

（５）第２のパスワード変更処理

図１０は、他のユーザの要求によるパスワード変更処理の説明図である。同図に示されるように、ユーザが、ユーザ端末１のパスワード変更依頼手段１４を用いて、認証ID[A1]とともに、ログインユーザ以外のユーザＩＤ（以下、他ユーザＩＤという。）[U2]、新パスワード[P2_6]を入力すると、ユーザ端末１は、認証サーバ２のパスワード変更手段２３に、認証ID[A1]、他ユーザＩＤ[U2]、新パスワード[P2_6]とともにパスワード変更を要求

する。
【００５２】
認証サーバ２のパスワード変更手段２３は、自身が保持する認証情報の中から、認証ID[A1]に紐付く、自ユーザＩＤ[U1]、自リビジョン[R1]、自パスワード[P1_1]から生成した鍵ハッシュ[Hk(P1_1)]を取得し、さらに[P2_6]から鍵ハッシュ[Hk(P2_6)]を生成する。次に、パスワード変更手段２３は、ユーザＤＢ３の鍵再暗号化手段３３に対して、ユーザＩＤ[U1]、自リビジョン[R1]、鍵ハッシュ[Hk(P1_1)]、他ユーザＩＤ[U2]、[Hk(P2_6)]を与え、マスター鍵[M]の再暗号化を要求する。
【００５３】
ユーザＤＢ３の鍵再暗号化手段３３は、ユーザＤＢ３が保持する鍵情報の中から、ユーザＩＤ[U1]、自リビジョン[R1]に紐付く、自暗号化済鍵[Ck(Hk(P1_1),M)]を取得し、鍵ハッシュ[Hk(P1_1)]を用いてマスター鍵[M]を復号する。また、[U2]に紐付くリビジョンのうち、最新の旧リビジョン[R5]を取得する。次に、鍵再暗号化手段３３は、鍵ハッシュ[Hk(P2_6)]を用いてマスター鍵[M]を暗号化し、生成された新暗号化済鍵[Ck(Hk(P2_6),M)]、他ユーザＩＤ[U2]、及び新リビジョン[R6]の組合せを鍵情報に新規追加する。
【００５４】
最後に、認証サーバ２のパスワード変更手段２３は、ユーザＤＢ３のユーザ情報記憶手段３１が保持するユーザ情報内に存在する、他ユーザＩＤ[U2]に紐付くリビジョン[R5]、パスワードハッシュ[Hp(P2_5)]を、鍵再暗号化手段３３から応答として受け取った[R6]、[P2_6]から生成したパスワードハッシュ[Hp(P2_6)]で上書更新し、パスワード変更依頼手段１４に応答する。
【００５５】
管理者などの上位ユーザが下位の一般ユーザのパスワードを変更するような場合に、他人に設定する新しいパスワードで鍵を暗号化する必要があるが、この鍵を自身のパスワードを用いて取得し、他人の新しいパスワードを使って暗号化を行い、他人が新しいパスワードを使用した際に鍵を取得できるようにしている。仕組は本人のパスワードを変更する場合（上記（５））と同じであり、処理の対象が他人のユーザ情報に変わるだけである。
【００５６】
（６）認証維持処理
図１１は、認証維持処理の説明図である。同図に示されるように、アプリケーションサーバ４の認証維持依頼手段４４は、定期的に、自機が保持する認証情報の中から、現在使用されているものを抽出し、対応する時刻を現在時刻で上書更新する。また、認証維持依頼手段４４は、定期的に、認証サーバ２の認証維持手段２４に、自機が保持する認証情報に含まれる認証ID（[A1]、[A2]）とともに認証維持を要求する。
【００５７】
認証サーバ２の認証維持手段２４は、アプリケーションサーバ４（認証維持依頼手段４４）から与えられた認証ID[A1]、[A2]と自機が保持する認証情報を突き合わせ、同一認証IDに紐付く時刻を現在時刻[T6]で上書更新し、認証維持依頼手段４４に応答する。
【００５８】
（７）鍵情報掃除処理
図１２は、鍵情報掃除処理の説明図である。同図に示されるように、認証サーバ２の鍵掃除手段２６は、定期的に、ユーザＤＢ３が保持する鍵情報の中から、古いリビジョンをユーザＩＤに紐付けて取得する。
【００５９】
次に、鍵掃除手段２６は、同サーバの認証情報確認手段２５及び他の認証サーバ２´（認証情報確認手段２５）のそれぞれに対して、取得したユーザＩＤと旧リビジョンの組（[U1],[R3]）、（[U1],[R4]）、（[U2],[R3]）が認証情報に含まれていないことの確認を要求する。
【００６０】
認証情報確認手段２５は、与えられたユーザＩＤと旧リビジョンの組と認証情報を突き

合わせ、存在の確認結果（[U1],[R3],true）、（[U1],[R4],false）、（[U2],[R3],false）を鍵掃除手段２６に応答する。

【００６１】

最後に、鍵掃除手段２６は、認証情報に存在しないことが判明した、ユーザＩＤと旧リビジョンの組（[U1],[R4]）、（[U2],[R3]）を鍵情報から削除する。過去のリビジョンの暗号化済鍵が使われなくなったことを確認してユーザＤＢ３から削除することで、不要になった古いデータがユーザＤＢ３内に保存され続けることを防ぐことができる。尚、他の認証サーバ２´においても同様の処理が行われるものとする。

【００６２】

（８）認証情報削除処理

図１３は、認証情報削除処理の説明図である。同図に示されるように、認証サーバ２（又はアプリケーションサーバ４）の認証削除手段２７（又は認証削除手段４５）は、定期的に、自機が保持する認証情報の中から、時刻が現在時刻から一定時間以上古い、すなわち、最後の認証から一定時間以上経過した情報を削除する。

【００６３】

以下、上記のように構成された暗号鍵管理システムの一連の動作を説明する。図１４は、一実施形態に係る暗号鍵管理システムにおけるパスワード変更時の動作の一例を示すシーケンス図である。

【００６４】

先ず、ユーザ端末１が、ユーザからの入力情報｛ユーザＩＤ＿１，パスワード＿１｝を認証サーバ２に送信し、認証要求を行う（Ｓ１０１）。

次に、認証サーバ２は、パスワード＿１に基づいて鍵ハッシュを作成し（Ｓ１０２）、保持している認証情報において同ユーザＩＤに関連付けられた最新リビジョン＿１の鍵ハッシュ＿１と比較する（Ｓ１０３）。比較結果が一致すると、認証サーバ２は、認証ＩＤ｛認証ＩＤ＿１｝をユーザ端末１へ返信する（Ｓ１０４）。

【００６５】

次に、ユーザ端末１は、認証ＩＤ｛認証ＩＤ＿１｝に基づいてアプリケーションサーバ４に接続要求を行う（Ｓ１０５）。

次に、アプリケーションサーバ４が、認証ＩＤ｛認証ＩＤ＿１｝に基づいて認証サーバ２に認証情報の参照を要求すると（Ｓ１０６）、認証サーバ２は認証ＩＤ｛認証ＩＤ＿１｝、リビジョン｛リビジョン＿１｝、鍵ハッシュ｛鍵ハッシュ＿１｝を含む認証情報を返信する（Ｓ１０７）。そして、アプリケーションサーバ４は、ユーザ端末１に接続完了を通知する（Ｓ１０８）。

【００６６】

次に、ユーザ端末１´が、同一ユーザからの入力情報｛ユーザＩＤ＿１，パスワード＿１｝を認証サーバ２に送信し、認証要求を行うと（Ｓ１０９）、認証サーバ２は、入力パスワード｛パスワード＿１｝に基づいて鍵ハッシュを作成し（Ｓ１１０）、保持している認証情報において同ユーザＩＤに関連付けられたリビジョン｛リビジョン＿１｝の鍵ハッシュ｛鍵ハッシュ＿１｝と比較する（Ｓ１１１）。比較結果が一致すると、認証サーバ２は、Ｓ１０４とは異なる認証情報｛認証ＩＤ＿２｝をユーザ端末１´へ返信する（Ｓ１１２）。

【００６７】

次に、ユーザ端末１´が、｛認証ＩＤ_２，パスワード＿２｝を含むパスワードの変更要求を認証サーバ２へ送信すると（Ｓ１１３）、認証サーバ２は、｛パスワード＿２｝による鍵ハッシュ｛鍵ハッシュ＿２｝を作成し、変更後のリビジョン｛リビジョン＿２｝および鍵ハッシュ｛鍵ハッシュ＿２｝をメモリ領域（図示省略する）に保持する（Ｓ１１４）。

【００６８】

次に、認証サーバ２は、ユーザＤＢ３に対して｛ユーザＩＤ＿１｝に関連付けられている｛リビジョン＿１，鍵ハッシュ＿１｝、｛リビジョン＿２，鍵ハッシュ＿２｝を送信し

、鍵再暗号化を要求する（Ｓ１１５）。従来技術との違いは、ここで新しいパスワードの鍵ハッシュ｛鍵ハッシュ＿２｝で復号できる暗号化済鍵を作成するだけでなく、古いパスワードの鍵ハッシュ｛鍵ハッシュ＿１｝で復号できる暗号化済鍵を残すことである。

【００６９】

次に、ユーザＤＢ３は、鍵再暗号化が完了すると、これを認証サーバ２へ通知する（Ｓ１１６）。すなわち、この時点では二つのユーザ端末１、ユーザ端末１´がそれぞれ異なる認証ＩＤで認証済みとなっている。

【００７０】

次に、最初に認証済みのユーザ端末１が、アプリケーションサーバ４に対してデータ参照を要求すると（Ｓ１１７）、アプリケーションサーバ４はデータサーバ５に｛リビジョン＿１，鍵ハッシュ＿１｝を送信し、データ読取を要求する（Ｓ１１８）。

【００７１】

次に、ユーザＤＢ３は、データサーバ５に鍵ハッシュ｛鍵ハッシュ＿１｝で復号可能な暗号化済鍵の送信を要求し（Ｓ１１９）、これをユーザＤＢ３が返信する（Ｓ１２０）。

【００７２】

次に、データサーバ５は、鍵ハッシュ｛鍵ハッシュ＿１｝により暗号化済鍵を復号してマスター鍵を取得し（Ｓ１２１）、このマスター鍵により保護データを復号して読取り（Ｓ１２２）、読取データをアプリケーションサーバ４へ送信する（Ｓ１２３）。

そして、アプリケーションサーバ４は、ユーザ端末１にデータ参照を開始させる（Ｓ１２４）。

【００７３】

このように、本実施形態に係る暗号鍵管理システムによれば、以下のような効果を奏する。

（１）認証されたユーザがシステムを利用している際に、並行してパスワードの変更があった場合でも、再認証を実行することなく、パスワード変更前のパスワードのリビジョンとユーザＩＤの組合せに係る暗号化済鍵によって保護データを継続して復号可能となる。例えば、ユーザ端末１が複数のアプリケーションサーバ４に接続されているような場合でも、アプリケーションサーバ４ごとに再認証を行う必要が無くなる利点がある。

（２）同一認証ＩＤの認証情報を利用中の他のユーザによってパスワードが変更された場合にも、認証済みのユーザは継続して保護データの登録・読取作業を行うことができる。

（３）古い鍵ハッシュに基づいて開始された処理に時間がかかる場合や、アプリケーションサーバの台数が多い場合であっても、パスワード変更による暗号関連情報の同期のために、再認証、ロック、処理完了待ち等が発生せず、操作性が向上する。

【００７４】

以上、本発明の実施形態を説明したが、本実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。この新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。本実施形態およびその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

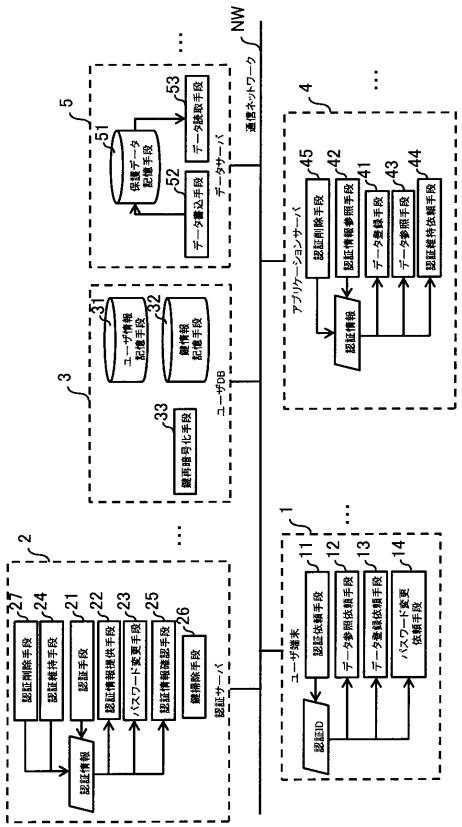
【符号の説明】

【００７５】

１…ユーザ端末、
２…認証サーバ、
３…ユーザＤＢ、
４…アプリケーションサーバ、
５…データサーバ、
１１…認証依頼手段、
１２…データ参照依頼手段、
１３…データ登録依頼手段、

１４…パスワード変更依頼手段、
２１…認証手段、
２２…認証情報提供手段、
２３…パスワード変更手段、
２４…認証維持手段、
２５…認証情報確認手段、
２６…鍵掃除手段、
２７…認証削除手段、
３１…ユーザ情報記憶手段、
３２…鍵情報記憶手段、
３３…鍵再暗号化手段、
４１…データ登録手段、
４２…認証情報参照手段、
４３…データ参照手段、
４４…認証維持依頼手段、
４５…認証削除手段、
５１…保護データ記憶手段、
５２…データ書込手段、
５３…データ読取手段。

【図１】



【図２】

認証情報

認証ID	ユーザID	リビジョン	鍵ハッシュ	時刻
A1	U1	R1	Hk(P1_1)	T1
A2	U1	R1	Hk(P1_1)	T2

【図３】

ユーザ情報

ユーザID	パスワードハッシュ	リビジョン
U1	Hp(P1_1)	R1
U2	Hp(P2_1)	R1
U3	Hp(P3_3)	R3

【図４】

鍵情報

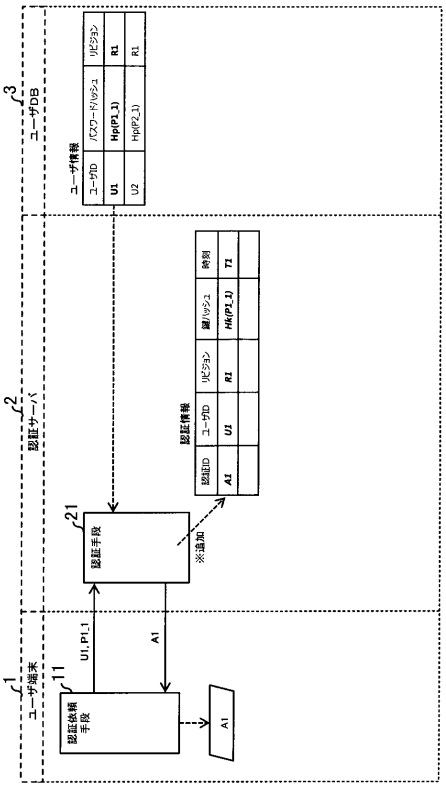
ユーザID	リビジョン	暗号化済鍵
U1	R1	Ck(Hk(P1_1),M)
U2	R1	Ck(Hk(P2_1),M)
U3	R3	Ck(Hk(P3_3),M)

【図５】

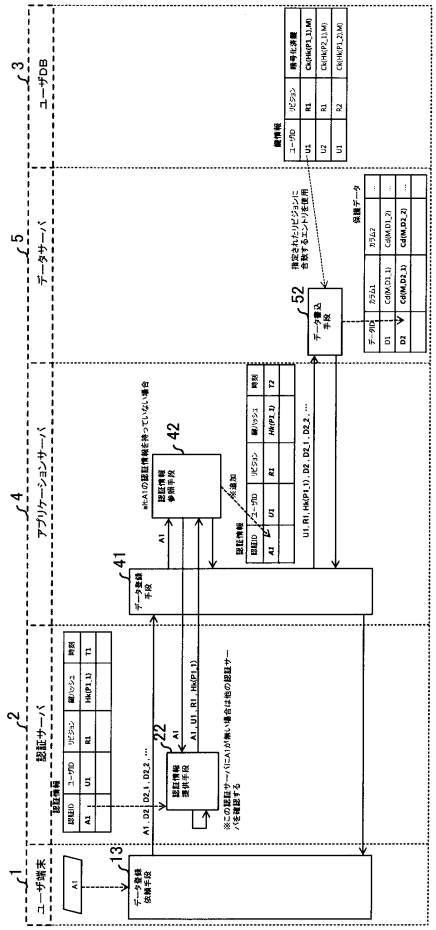
保護データ

データID	カラム1	カラム2	...
D1	Cd(M,D1_1)	Cd(M,D1_2)	...
D2	Cd(M,D2_1)	Cd(M,D2_2)	...
D3	Cd(M,D3_1)	Cd(M,D3_2)	...

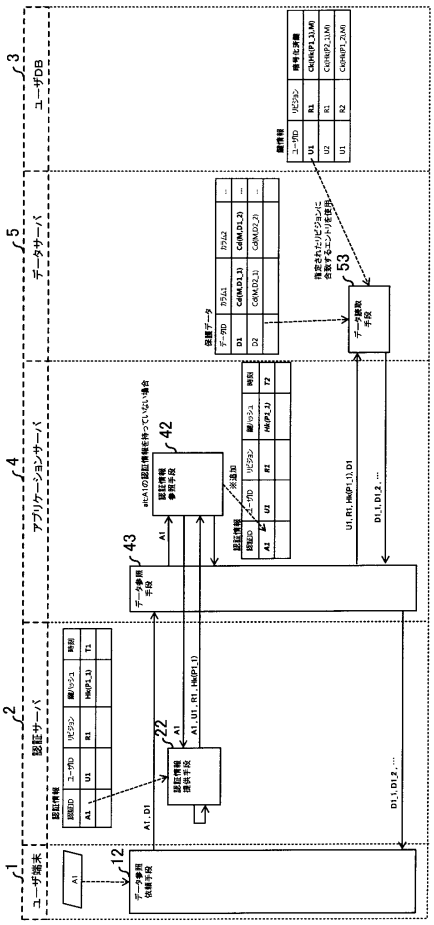
【図６】



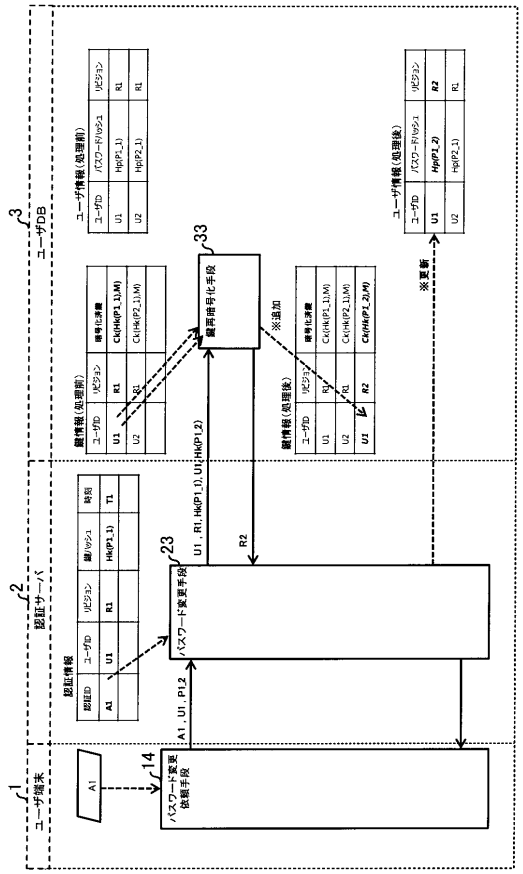
【図７】



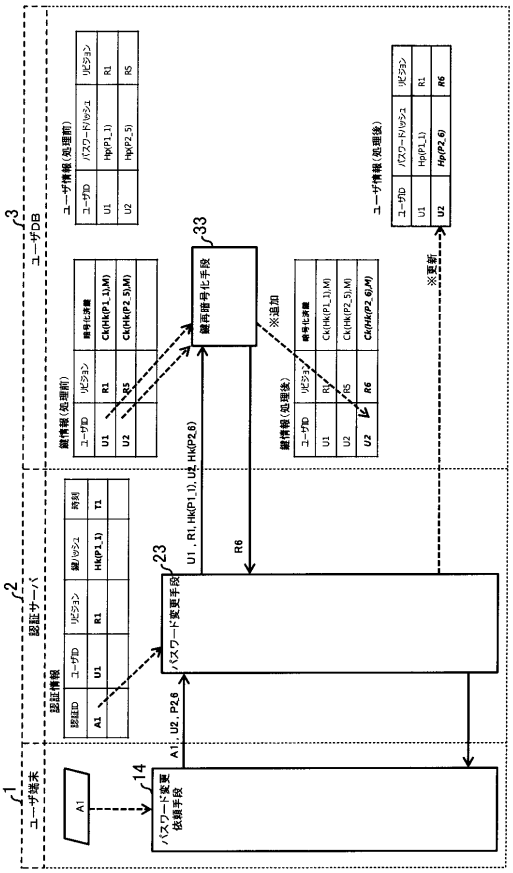
【図８】



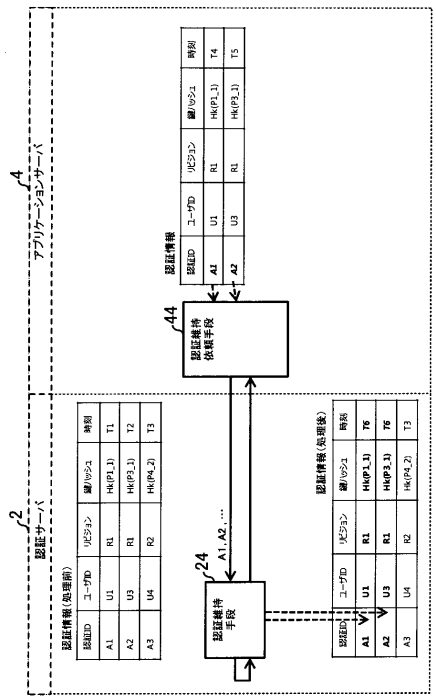
【図９】



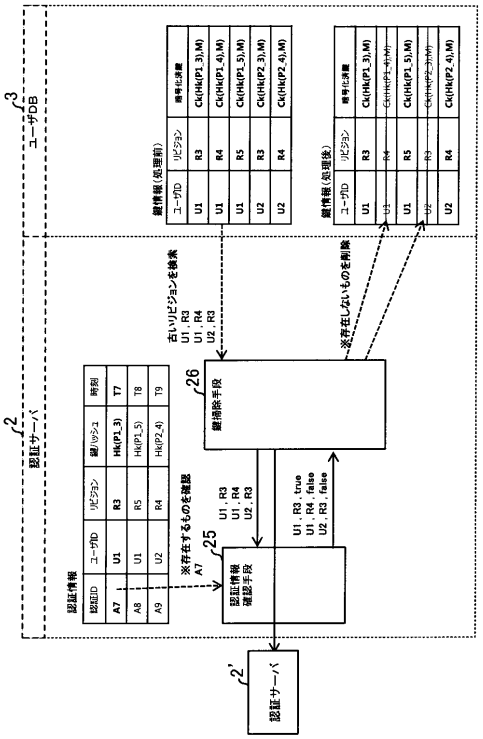
【図１０】



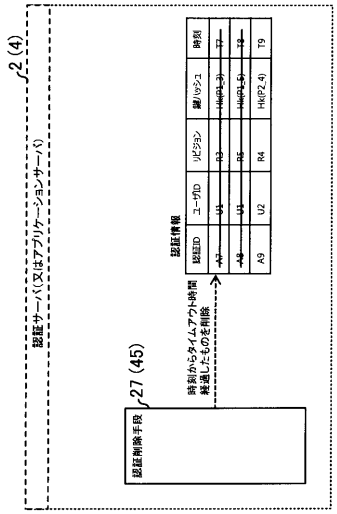
【図１１】



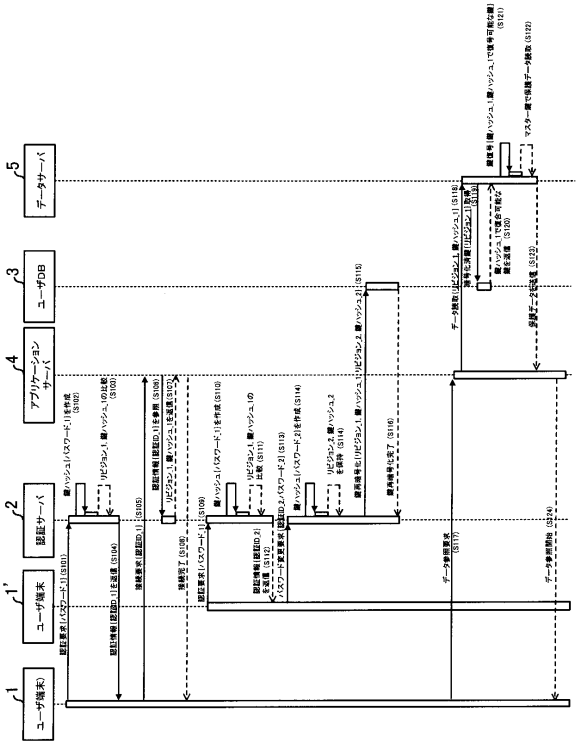
【図１２】



【図１３】


2 (4)
認証サーバ(又はアプリケーションサーバ)
27 (45)
認証削減手段
時刻からタイムアウト時間経過したものを削除
認証情報
認証ID
ユーザID
リビジョン
鍵ハッシュ
時刻
A7
U1
R3
HH(P1-3)
T7
A8
U1
R5
HH(P1-5)
T8
A9
U2
R4
HH(P2-4)
T9

【図１４】


1 ユーザ端末
1' ユーザ端末
2 認証サーバ
3 ユーザDB
4 アプリケーションサーバ
5 データサーバ

フロントページの続き

(51)Int.Cl.　　FI
　　H04L　9/00　　641

(72)発明者　青木　翼
　　神奈川県川崎市幸区堀川町７２番地３４　東芝ソリューション株式会社内

審査官　行田　悦資

(56)参考文献　特表２００１－５１６９１３（ＪＰ，Ａ）
　　特開２００８－２５７６９１（ＪＰ，Ａ）
　　特開平０５－０３０１０３（ＪＰ，Ａ）
　　特開２００６－２６８７１９（ＪＰ，Ａ）
　　特開２００５－０６３４３９（ＪＰ，Ａ）
　　特開２００２－００９７５４（ＪＰ，Ａ）
　　特開２０１１－２５６５６１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
　　Ｈ０４Ｌ　　９／０８
　　Ｇ０６Ｆ　２１／３１
　　Ｇ０６Ｆ　２１／６２
　　Ｈ０４Ｌ　　９／１４
　　Ｈ０４Ｌ　　９／３２